Инструкция по настройке подписания документов в системе CyberFT с помощью сервиса (CyberFTSignService)

Программное обеспечение **CyberFTSignService** представляет собой локальный сервис, работающий в виде службы на компьютере подписанта и служит для связи между Терминалом CyberFT и сервисами криптографии Windows.

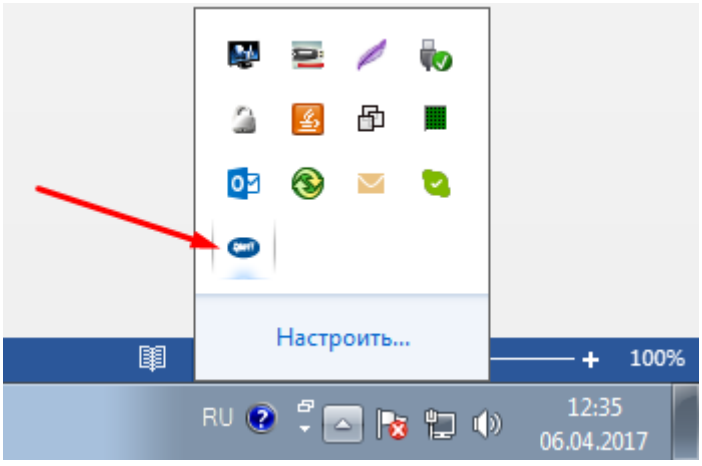
ПО CyberFTSignService доступно по ссылке: http://download.cyberft.ru/CyberSignService/
Сохраните локально наиболее актуальный архив, разархивируйте и запустите установку с **правами администратора.**

При установке служба автоматически добавится в автозагрузку Windows.

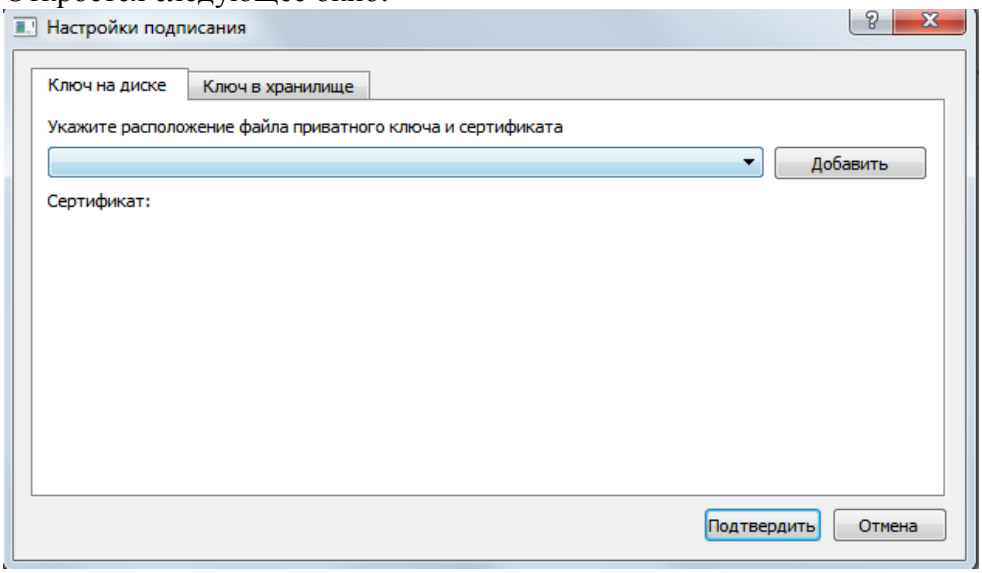
Настройка ключей для подписания

По завершению установки, необходимо настроить ключи для подписания, для этого выполняем действия описанные ниже.

1) Находим значок программы в трее и кликаем левой кнопкой мыши



Откроется следующее окно:



Далее внимательно прочтите инструкцию с описанием вариантов настроек и выберите наиболее подходящий вам.

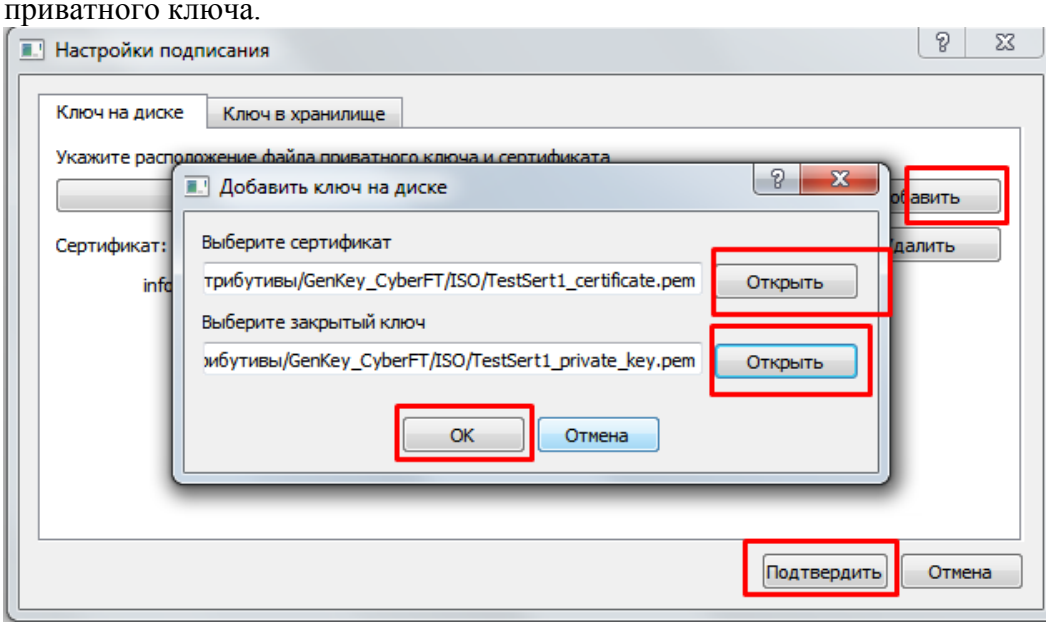
Вариант 1: Подписание ключами на диске.

Если сертификат и закрытый ключ находятся на локальном диске или flash носителе, то настройка производится на первой вкладке **Ключ на диске.**

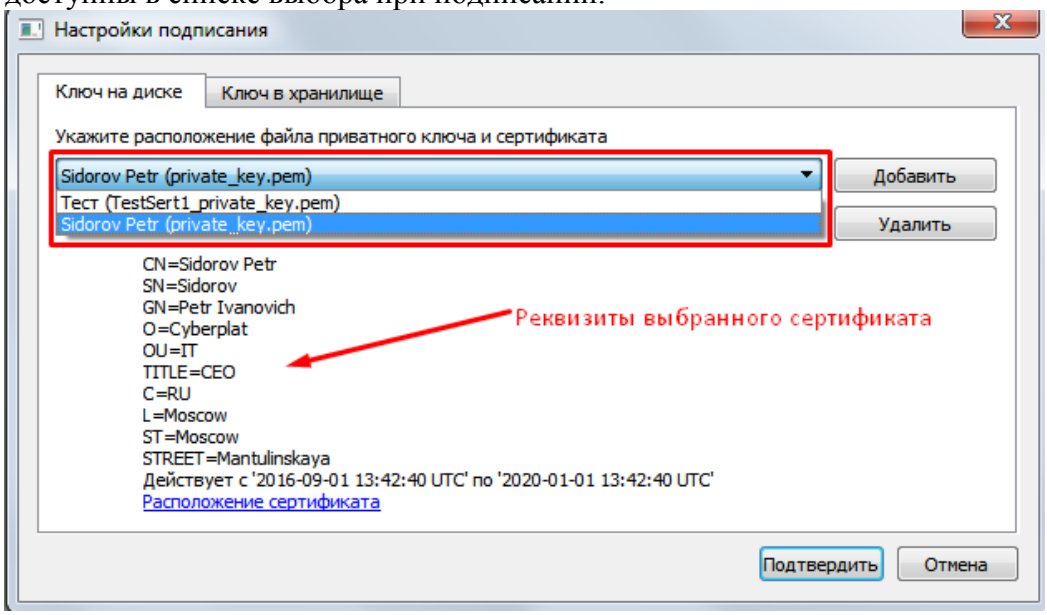
Данная настройка удобна в случае, если планируется подписание несколькими ключами подписанта на одном компьютере т.к. позволяет в момент подписания выбирать нужный сертификат.

Предполагается что файлы приватного ключа и сертификата были ранее получены посредством генерации в ПО GenKey.

Нажимает **Добавить** и в открывшемся окне указываем путь к файлу сертификата и приватного ключа.



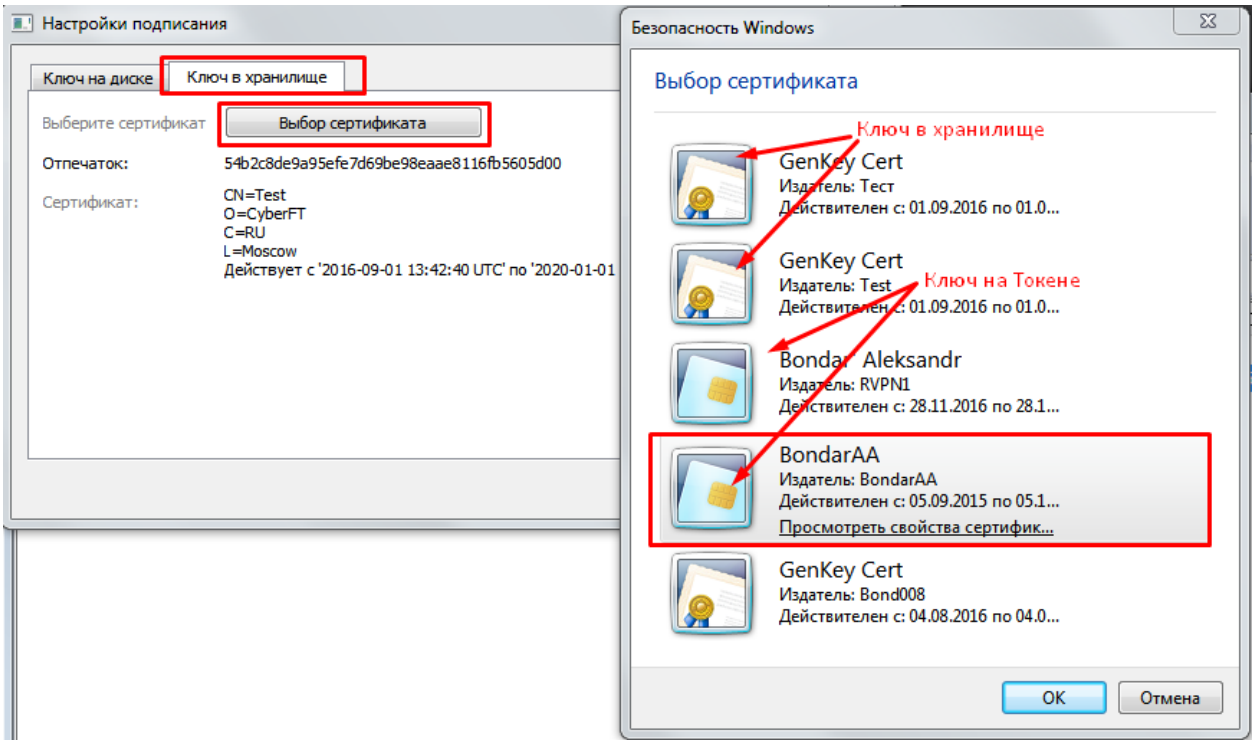
Таким образом можно добавить несколько ключей подписантов после чего они будут доступны в списке выбора при подписании.



Вариант 2: Подписание ключами на токене

Если ключи расположены на Токене, то переходим на вкладку Ключ в хранилище.

Выбираем сертификат на Токене (нужный токен должен быть вставлен в USB порт)



Далее при подписании будет происходить обращение к выбранному ключу.

Пользователь при подписании вводит пароль на Токен

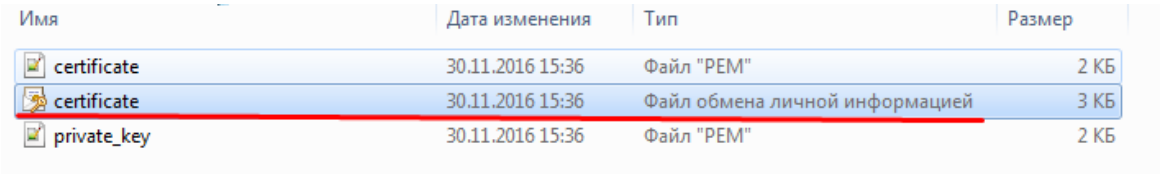
Чтобы подписать документ другим ключом необходимо заново открыть настройку и выбрать другой сертификат.

Вариант 3: Подписание ключом из Хранилища Windows

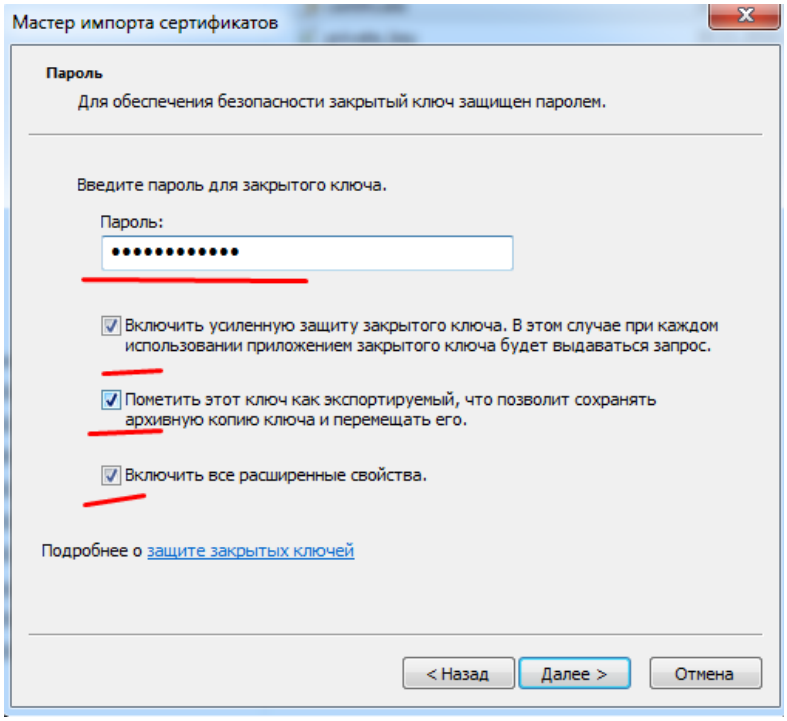
Данный вариант удобен если пользователь пользуется для подписания в CyberFT только одним ключом и при этом нет возможности записать ключ на Токен.

При генерации комплекта ключей через ПО GenKey создается файл ключевого хранилища certificate.pfx
Сертификат и закрытый ключ из данного хранилища PFX можно импортировать в хранилище Windows и использовать далее при подписании документов.

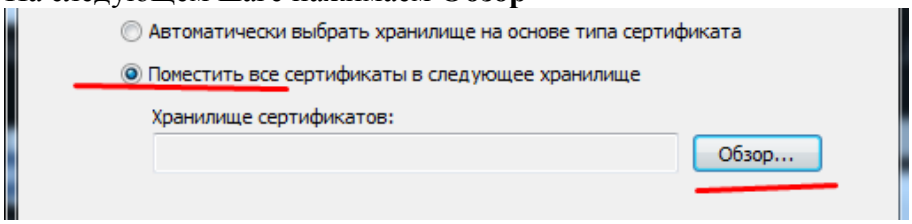
Добавим сертификат и закрытый ключ в хранилище Windows.
Открываем файл хранилища ключей (с расширением PFX) из комплекта созданных посредством GenKey ключей.



Ставим галочки в чекбоксы отмеченные на скрине, вводим пароль, указанный при генерации ключа и нажимаем **Далее.**



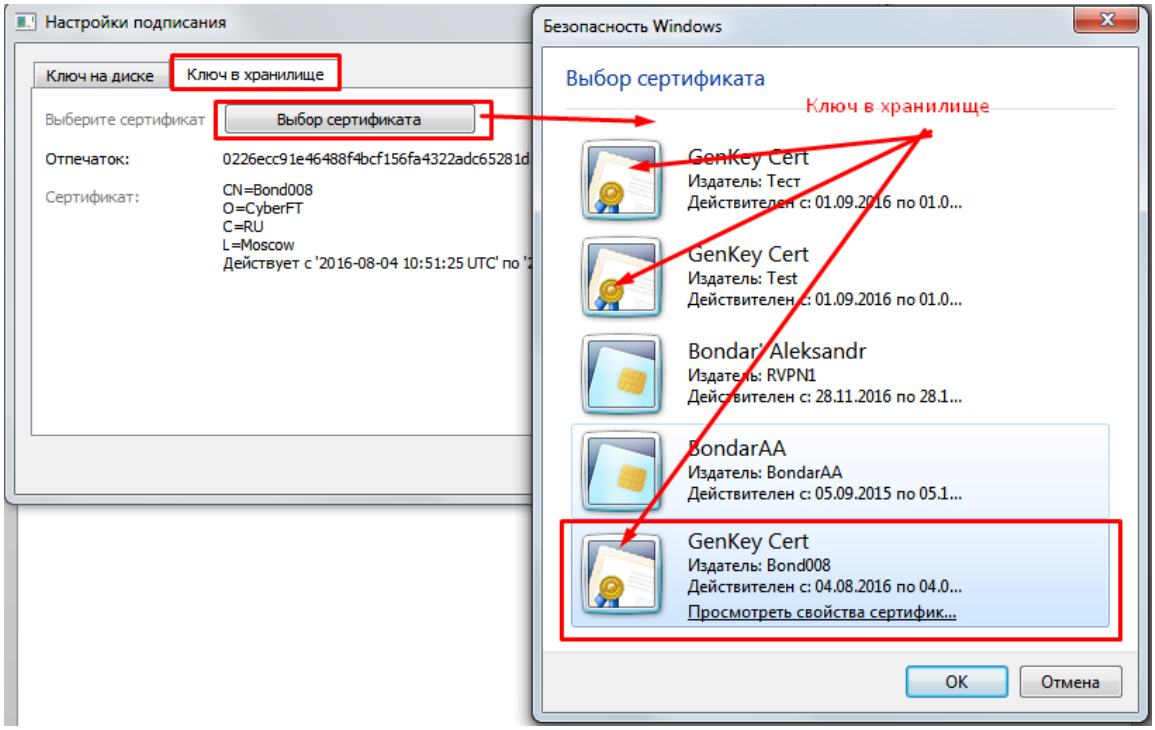
На следующем шаге нажимаем **Обзор**



Выбираем **Личное** хранилище сертификатов и нажимаем **Готово**.

Если появится окно безопасности, нажимаем «**ОК**»

Далее открываем настройку сертификатов сервиса CyberFTSignClient и выбираем добавленный в хранилище сертификат.



По окончании выбора нажимаем кнопку **Подтвердить**

При подписании документа Пользователю не предоставляется выбор сертификата. По умолчанию при подписании будет использоваться выбранный ключ.

При подписании пользователь вводит пароль от закрытого ключа указанный при генерации в GenKey.